OPIC
Office de la propriété
intellectuelle du Canada

CIPO
Canadian Intellectual
Property Office

Ottawa Hull K1A 0C9

(21) (A1) 2,153,281
(22) 1995/07/05
(43) 1996/01/09

(51) Int.Cl.^{6} H04L 12/12

(19) (CA) **APPLICATION FOR CANADIAN PATENT** (12)

(54) Mediated Access to an Intelligent Network

(72) Schwartz, Ronald - Canada ;
Turner, Douglas Gordon - Canada ;
Archambault, Sylvain - Canada ;
Mufti, Sohale Aziz - Canada ;
Rainey, Gordon Lester - Canada ;
Stanke, Marianne Jo - U.S.A. ;
Heinmiller, Wayne Robert - U.S.A. ;
Shook, LaVerne Bentley - U.S.A. ;
Schoenstedt, Robert Curtis - U.S.A. ;
Hull, Marie-Ellen - U.S.A. ;

(71) Same as inventor

(30) (US) 08/272,207 1994/07/08

(57) 29 Claims

Notice: This application is as filed and may therefore contain an incomplete specification.

MEDIATED ACCESS TO AN INTELLIGENT NETWORK

Abstract of the Disclosure

A network service access system and method for intelligent networks uses a network element called a mediation point between network service switching points (SSP) and third party service provider service control points (SCP). The mediation point acts as a gateway to the AIN network for the service provider SCPs. The mediation point at the boundary of the intelligent network has ports for connection to service providers SCPs and a list of SSPs within the intelligent network to which each respective service provider is allowed access.

MEDIATED ACCESS TO AN INTELLIGENT NETWORK

This invention relates to intelligent networks and is particularly concerned with providing mediated access to intelligent networks for service providers.

Background to the Invention

The Intelligent Network (IN) architecture has been evolved through the efforts of groups, in particular Bellcore, European Telecommunications Standards Institute (ETSI), International Telecommunications Union (ITU-T), and American National Standards Institute (ANSI). These groups have issued respective documentation defining general architecture for IN. This evolution is being driven by the increasing demand for rapid and responsive deployment of services on the telecommunications network.

Increasing competition and changing regulations are providing both a challenge and an opportunity to the telecommunications industry. While some interconnections between network providers have existed for a decade or more, and Open Network Architecture (ONA) rules and capabilities have been and continue to evolve, new technologies are increasing the sophistication of these interconnections and hence both their value and their power.

In 1992, the Federal Communications Commission (FCC) mandated the Information Industry Liaison Committee (IILC) to begin work on defining the requirements for network unbundling such that other Service Providers could obtain intelligent access to local subscribers through the LEC network. In addition, in 1993, the FCC issued a Notice of Proposed Rulemaking (NPRM) on Common Carrier Docket 91-346, to gather industry views on the requirements for regulations regarding the opening of LEC networks at the SCE, SMS, SCP and CSP levels.

To date, service provider access has been technologically difficult to achieve as services have been based on proprietary switches. With intelligent networks (IN), there is an opportunity to provide an open/standard interface whereby service logic in a service control point

(SCP) is separated from the switches, (called service switching points (SSPS) in IN).

Initially, the Local Exchange Carriers (LECs) did not intend to use advanced intelligent network (AIN), as defined by Bellcore, to allow competition for services business, but soon recognized this as a new business opportunity. The FCC is aware that there are technology issues that have to be resolved, especially how to protect the integrity/reliability/security of the public switch networks if the intelligent networks are unbundled.

Summary of the Invention

An object of the present invention is to provide improved access to intelligent networks for service providers.

In accordance with an aspect of the present invention there is provided a method of providing mediated access to an intelligent network for service providers, the method comprising the steps of: providing a mediation point at a boundary of the intelligent network for connection to the service providers; providing, at the mediation point, a predetermined list of network nodes in the intelligent network to which respective service providers are allowed access; screening, at the mediation point, a message between a service provider and a network node connecting a subscriber of the service provider to ensure that the network node is on the predetermined list of network nodes the service provider is allowed to access in the intelligent network; and subsequently, routing messages between the service provider and the network node.

In accordance with another aspect of the present invention there is provided a system for providing mediated access to an intelligent network for service providers, the system comprising: a mediation point at a boundary of the intelligent network having ports for connection to service providers and a predetermined list of network nodes in the intelligent network to which respective service providers are allowed access; and a plurality of network nodes for connecting subscribers, each having trigger criteria, for each service provider having access thereto, for selecting one of the service providers in response to a subscriber.

In accordance with a further aspect of the present invention there is provided a method of providing mediated access to an intelligent network for service providers, the method comprising the steps of: ensuring that network integrity, security, and reliability are protected in giving a service provider access to the intelligent network; allowing the service provider access to the intelligent network; and billing the service provider for gaining access to the intelligent network.

In accordance with yet another aspect of the present invention there is provided a system for providing mediated access for service providers to an intelligent network, the system comprising: a mediation point at a boundary to the intelligent network and having mediation functions for interconnection of service provider service control points to predetermined service switching points within the network; and service switching points within the network having mediation functions for interconnection to selected service provider service control points.

An advantage of the present invention is it provides a clear physical boundary point with non-LEC service providers, standard SS7 signalling, and access to Advanced Intelligent Network (AIN) trigger points. The mediation point becomes the key platform on which specific mediation functions are located, and it can be customized to the requirements of individual network providers.

The service switching point (SSP) is enhanced with functions that are tightly coupled to the AIN Basic Call Model, and all management of trigger-specific data remains at the SSP, as per general AIN philosophy. Thus, overall AIN definition is grown in a consistent fashion and impacts to implement and deploy mediated access are minimized.

Brief Description of the Drawings

The present invention will be further understood from the following description with reference to the drawings in which:

Fig. 1 illustrates an intelligent network (IN) with mediated access points;

Fig. 2 illustrates in a block diagram an advanced intelligent network (AIN) system with mediated access in accordance with an embodiment of the present invention;

Fig. 3 illustrates in a block diagram distribution of mediation functions in the system of Fig. 2;

Fig. 4 illustrates in a block diagram message flow for normal trigger processing between mediation functions in the system of Fig. 2;

Figs. 5 illustrates in a block diagram message flow for unsolicited messages between mediation functions in the system of Fig. 2;

Fig. 6 illustrates in a block diagram message flow for overload management between mediation functions in the system of Fig. 2; and

Fig. 7 illustrates in a block diagram the mediation point of Fig. 2 in accordance with an embodiment of the present invention.

Similar references are used in different figures to denote similar components.

Detailed Description

Referring to Fig. 1 there is illustrated an intelligent network (IN) with mediated access points.

The intelligent network, represented by cloud 10 provides all of the interconnection service between access subscribers 12. Service providers, as represented by broken line rectangle 14, desiring access to the intelligent network are connected via mediated access 16 and 18. The mediated access 16 connects a service control point (SCP) 20 to the intelligent network 10. The mediated access 18 connects a service management system 22 of service provider 14 to the intelligent network 10. Where to locate such mediated access and how to implement the mediated access functions presents several problems related to balancing costs, deployment time and quality of service. Also the concerns of network operators, service providers and subscribers must be met by the mediated access.

Referring to Fig. 2, there is illustrated in a block diagram an advanced intelligent network (AIN) system with mediated access in accordance with an embodiment of the present invention.

The intelligent network includes service switching points (SSP) 30, each logically connected to signal transfer points (STP) 32 and an intelligent peripheral (IP) 34. The intelligent network is enhanced with the addition of a network element, a mediation point 36 in accordance with an embodiment of the present invention. The mediation point 36 is logically connected to the STP 32. The mediation point 36 is logically connected to service provider SCP 38.

Providing mediated access into the AIN also includes mediation functions at the SSP 30, as represented by a hexagon 40.

In order to provide mediated access to the AIN for service providers, mediation functions must be distributed among the network elements of Fig. 2.

Referring to Fig. 3, there is illustrated in a block diagram distribution of mediation functions in the system of Fig. 2.

Fig. 3 shows the same network elements as Fig. 2, and also includes a network management system 42 (not shown in Fig. 2). Connection of the network management system 42 to the system is not shown, but is well known in the art. Fig. 3 shows the distribution of mediation functions among the network elements, the functions grouped within broken line rectangles associated with the network element performing the function.

Most of the mediation functions reside in the mediation point 36. These functions include screening 44, billing 46, error handling 48 and routing 50. Specific examples of each of these types of functions are:

For screening 44,

- MTP (message transfer part) screening
- SSP screening
- Parameter screening (to and from SCP)
- RPCU (radio port control unit) ID screening
- Record received message errors

For billing 46,

- Trigger queries
- NCA (Non-Call Associated) messages
- Dynamic trigger arm/disarm

For error handling 48,

- Babbling SCP detection/control and

For routing 50,

- MP SCCP (signal connection and control part) procedures
- Route messages.

The service switching point (SSP) 30 also includes some mediation functions as indicated by the hexagon 40. These functions include routing 52, billing 54, screening 56 and error handling 58. Specific examples of each of these types of functions are:

For routing 52,

- Service provider selection per trigger
- SSP SCCP procedures
- Route messages to mediator
- Emergency service routing

For billing 54,

- ACG (automatic call gapping) usage

For screening 56,

- ACG to allowed users
- Trigger arm/disarm and

For error handling 58,

- Custom T1 value
- Default on T1 expiry
- ACG default

The remaining network elements, the signal transfer point (STP) 32 and the intelligent peripheral (IP) 34 provide routing 60 and billing 62 functions, respectively, used to provide the mediation service. The network management system 42 provides network level error handling 64. Specific examples of these functions are:

For STP routing 60,

- Route messages

For IP billing 62,

- Custom announcements and

For the network management system error handling 64

- Control network overload

Operation of the system of Fig. 2, is described hereinbelow in conjunction with Figs. 4, 5 and 6.

Referring to Fig. 4, there is illustrated in a block diagram message flow for normal trigger processing between mediation functions in the system of Fig. 2.

Subscriber 70 initiates an AIN trigger activity based on normal AIN trigger event criteria, which can happen on call originations and terminations. Service provider ID is in the trigger data, as subscribed. The mediation function represented by hexagon 40 within the SSP 30 begins the process by a 1) select service provider. Each trigger instance is associated with exactly one service provider. When trigger criteria are met, the service provider's SCP 38 is selected. The process at the SSP 30 next carries out 2) SCCP procedures. The SCCP procedures use global title routing on all SSP messages which are part of a trigger conversation, response to an SCP-initiated transaction, or are unidirectional.

In a received message, the SCCP calling party address, which must include the global title address (GTA) of the SCP 38, is placed in the SCCP called party address field of the outgoing message. For conversation messages in the context of a trigger transaction, the GTA can also be taken from the trigger instance data. For unidirectional messages, the GTA is available from a previously terminated transaction (e.g. for an error message), or identified by the RPCU for non-call associated messages.

The next process step at the SSP 30 is 3) T1 set.

The last process step performed by the SSP 30 is 4) routing query to MP. The GTA of the service provider's SCP (whether duplicated or not) is associated with the trigger instance. When trigger criteria are met, and the trigger is armed, the SCP's GTA is included in the SCCP called address field of the outgoing query. Based on an outstanding ACG request, the query may be rejected, in which case default action may be taken.

The SSP 30 uses as input data GTA of service provider's SCP in each trigger instance and, if applicable, ACG data for targeted users and SSPs for each SCP. The output of the SSP 30 routing step is in GTA in the query's SCCP called address field. The STP 32, passes the query from the SSP 30 to the MP 36 in 5) routes query to MP.

The mediation point (MP) 36 begins its mediation process with 6) parameter screening. Based on the service provider profile and general privacy requirements, certain parameters are not included in outgoing AIN query messages, regardless of the availability of the information.

Disallowed parameters are removed from the AIN Message sent by the SSP 30. For subscribed parameters where the data is private (i.e. restricted numbers), only the private data is removed; the rest of the parameter is left intact. The MP 36 uses a list of allowed parameters, and values, per SCP for outgoing messages, to screen the message from SSP 30 to provide a filtered AIN message. Call processing data may be used by the MP 36 to assist this screening.

The next step for MP 36 is to initiate 7) trigger query billing. Every time a trigger's criteria are met, and a query is originated, a record may be made for usage-sensitive billing purposes.

The MP 36 performs an SCCP procedure 8). The SCCP procedure represents a change introduced by mediation into the normal SS7/AIN model. The SSP 30 must be able to address both the MP 36 and SCP 38, while the SCP 38 must address both the MP 36 and SSP 30. The additional need to address the MP 36 on all messages, in both directions, is the reason for these new procedures.

After performing 8) SCCP procedures, the MP 36, 9) routes query to SCP 38. The MP 36 includes global title address (GTA) of the SSP 30 for messages sent on to the SCP 38.

In a received message, the GTA in the SCCP calling party address field is placed in the outgoing message.

Using SCCP information in received messages from the SSP 30 or SCP 38, the MP 36 provides SCCP information in outgoing messages, and makes a peg count of messages missing SCCP global title address.

The service provider's SCP 38 performs whatever processing is appropriate with step 10) feature processing and generates with step 11) a response to the SSP 30.

On receiving a response from the SCP 38, MP 36 performs several screening steps. In step 12) message transfer part (MTP) screening, the MP 36 screens messages from service providers to ensure: the origination point code (OPC) is that of the connected SCP; the destination point code (DPC) can only be that of the MP. The impact is that messages must be processed by the mediation application at the MP, and the SCP can not misrepresent itself.

The OPC must be allowed over the SS7 link-set, that is, it must identify the SCP 38. The DPC screening is provided by known STP Gateway screening.

In step 13) SCCP screening, the MP 36 performs SCCP called party address screening that ensures the SCP addresses only authorized SS7 nodes, including SSPs.

Each message from an SCP (query, conversation, response, unidirectional) is screened. The global title address in the SCCP called party address field is screened against a list authorized SS7 nodes. SCP messages must include the GTA of both the SCP 38 and SSP 30. These procedures ensure proper SCCP addressing on subsequent messages. Messages from the SCP must include the GTA of the SCP in the SCCP calling party address and the GTA of the SSP in the SCCP called party address. If a message received at the MP 36 does not include this global title information, it is ignored, and the occurrence is pegged. The message is ignored if screening fails.

The MP 36 may perform other screening, for example, TCAP (transaction capabilities application part) and AIN message screening. After normal TCAP and AIN Message screening (both response and unsolicited messages), if an error is found the screening failure is pegged and the message is logged. The erroneous message is then discarded.

As shown in step 15), the MP 36 performs parameter screening. Each parameter in the response message is checked against the list of allowed parameters. If a parameter is allowed, the contents are checked against the list of allowed values, if applicable. If screening fails, the message from the SCP 38 is discarded, but the screening failure is pegged.

Step 16) SCCP procedures and 17) route response to STP are similar to steps 8) and 9) described hereinabove.

The STP 32 in step 18) routes the response from the SCP 38 to the SSP 30. To complete the exchange, SSP 30 in step 19) processes the trigger response in a manner as is known in AIN.

Referring to Fig. 5, there is illustrated in a block diagram, a message flow for unsolicited messages between mediation functions in the system of Fig. 2.

In the system of Fig. 2, the SCP 38 may, in providing a service to the subscriber 70. after a step of 1) feature processing, send an unsolicited message, step 2) to the MP 36.

The MP 36 performs the screening steps 3), 4), and 5) as in Fig. 4 steps 12) 13) and 14). In addition, the MP 36 may perform dynamic arm/disarm screening and Radio Port Control Unit (RPCU) screening for personal communication services (PCS) step 6).

Based on service provider subscription, NCA (Non-Call Associated) messages from the SCP 38 intended for an RPCU (Radio Port Control Unit - for PCS) 72 must be authorized.

If an AIN message from the SCP 38 contains an RPCU Id of a destination RPCU 72, it is checked against an SCP-specific list of allowed RPCU Ids. If screening fails, the message is ignored, and the screening failure is pegged.

For unsolicited messages, the MP 36 may generate a billing record at step 7).

The service provider may be billed for every request to dynamically arm or disarm a previously provisioned trigger.

The remaining steps in Fig. 5 are the same as similarly worded steps in Fig. 4, performed by the same network element.

In step 11) the SSP 30 in processing the unsolicited message performs screening of trigger arm/disarm messages from the SCP 38. If an AIN message from the SCP 38 is a trigger arm or disarm request, the target user and trigger are checked to see that it exist and that the SCP associated with the user's trigger equals that of the SCP making the request. If screening fails, the request is rejected and the SCP 38 is informed.

The SSP 30 also checks automatic call gapping (ACG) messages from the SCP 38. If an ACG request is received from the SCP 38, the SSP 30 checks each query for the associated SCP before applying ACG controls. The SSP 30 must store the SCP identification, with each ACG request, to support this function.

At step 12), the SSP 30 generates a billing record for ACG requests. ACG requests from SCP 38 are billed according to the scope of each request's network impact. This includes the number of SSPs and users impacted, and the duration for the gapping process.

When the intelligent peripheral (IP) 34 is invoked in providing service, for example for announcements, a billing record is generated by the IP 34. Every time a custom announcement is to be played, a record may be made for usage-sensitive billing purposes. A "Send-To-Resource" response from the SCP 38 which corresponds to a custom announcement at the IP 34, initiates the billing action.

Referring to Fig. 6, there is illustrated in a block diagram, a message flow for overload management between mediation functions in the system of Fig. 2. Fig. 6 illustrates, by way of example, how overload management may be handled.

When the SS7 network becomes overloaded, remedial action is taken by the network by reducing traffic. The network reduces traffic in the following order (increasing severity) until the overload is remedied. As network surplus capacity returns, the remedial actions are stopped, in reverse order.

1) Mass Calling
2) Overloaded SCPs
3) SCPs exceeding traffic thresholds
4) Uniformly, for all traffic on overloaded network resources.

Fig. 6 also shows examples of how the network elements deal with error conditions. For example, the MP 36 detects and controls babbling SCPs. A babbling SCP is one sending nonsense messages into the network which may cause network problems and hence must be detected and rectified quickly. The network monitors compliance with predetermined, expected service provider SCP TCAP traffic levels and takes remedial action if levels are exceeded.

The SSP 30 is also involved in error detection and recovery. For example, if the T1 timer expires, default action can be an announcement or continue routing on the dialed number or a default number.

When a query is sent to the SCP 38, the T1 timer is started (see Fig. 4, step 3). If the timer expires, or the SCP response is ignored due to screening, the default announcement or routing is taken, based on the trigger instance data. Network management is notified of T1 expiry.

The SSP 30 may, for example, take default action with regard to an existing ACG request. An existing ACG request from the SCP 38 causes the SSP 30 to abort the trigger query; subsequent handling is the same as if the query had been sent and the T1 timer expired. Default action is identical to that for T1 expiry, except network management is not notified.

Referring to Fig. 7, there is illustrated in a block diagram the mediation point 36 of Fig. 2 in accordance with an embodiment of the present invention. The mediation point (MP) 36 includes a network interface 100, a high-speed bus or local area network (LAN) 102 and multiple query processors 104 and a service provider (SP) interface 106. Each query processor (QP) 104 includes storage media 108 and 110 for retaining data related to service provisioning. The network interface 100, the query processors 104 and the service provider (SP) interface 106 are interconnected via the high-speed bus or LAN 102. The network interface 100 is connected to service switching points in the network via SS7 network links 112. The service provider interface 106 is connected to service provider via links 114.

The MP 36 is an example of a loosely-coupled architecture in which each processor is a self-contained computer system having local memory, disk drives and other I/O devices. The query processors 104 communicate with one another by sending messages across the high-speed bus or LAN 102.

An SSP 30 generates a normal AIN trigger query message, which is routed to the MP (message 1) 122. Using normal SS7 processing in the network interface 100, the MTP layer hands message off to the SCCP layer for further translation, which determines that the message requires application layer work at the MP. This is communicated (message 2) 124 to the appropriate query processor 104a and the mediation application is identified by the SCCP sub-system number (SSN).

The QP 104 has access to the full SS7 message 124, including the MTP 126 and SCCP 128 layers. The QP 104 performs the applicable screening and billing functions, referring to service provider profile and other supporting data in its associated data bases 108 and 110. The QP 104 sends the resulting message for SS7 routing (message 3) 130 to the service provider interface 106. At the service provider interface 106, normal SS7 processing determines (from the SCCP information) that the message is destined for the SCP 38, and transmits it (message 4) 132 across the network boundary 134 toward the service provider SCP 38.

The service provider SCP 38 processes the AIN message based on each user's subscription information and service logic, as arranged with their users. Once feature processing is completed, the results must be indicated to the SSP 30. The SCP 38 sends a response (message 5) 136 across the network boundary 134 to the MP. At the service provider interface 106, SS7 processing occurs as described above for the network interface 100. This results in sending of the message (message 6) 138 to a QP 104. The selected QP 104h has access to the full SS7 message 138, including the MTP 140 and SCCP 142 layers. The QP 104h performs the applicable screening, billing and error handling functions, referring to the service provider profile and other supporting data in its associated databases 108h and 110h. If the message is not rejected, the QP 104h sends the resulting message (message 7) 144 for SS7 routing to the network interface 100. At the network interface 100, normal SS7 processing determines (from the SCCP information) that the message is destined for the SSP 30, and transmits it (message 8) 146.

From this point, after subsequent normal SSP AIN message processing, further communication between the SSP 30 and SCP 38 may occur, and the operation of all elements shown is the same as described above. This is also true for SCP-initiated transactions and unidirectional messages.

QPs 104 can be added as load dictates, for the most economical deployment.

For each message, whether from the SSP 30 or SCP 38, any QP 104 can be selected. It need not be the same one as used for any other message, including other messages which are part of the same AIN transaction. Each QP 104 has access to the same databases of information, either by using the same instances of databases 108 and 110, or by duplicating the databases for each QP 104.

Once the MP has sent the message to the SCP 38 or SSP 30, no data regarding the transaction needs to be retained, and dynamic resources can be reused for processing of other messages. In this way, the MP supports full routing diversity for all AIN messages. That is, like an STP, any MP could handle any message. This allows maximum flexibility in network topology. An MP failure during a transaction will not cause a transaction failure if no messages are lost.

The mediation functions of the present invention are directed toward the AIN 0.1 and 0.2 releases of AIN as defined by Bellcore. The present invention provides a foundation for not only mediating access to 0.1 and 0.2 AIN capabilities, but also to those which are certain to arise in future releases, as long as the clear separation between SSP (basic call model) and SCP (service logic) is maintained. If the signalling between the SSP and the service logic element (which may not always be a pure SCP element) is something other than SS7 (e.g. X.25, Ethernet) the present invention still provides the types of functions located at the SSP and MP, and how the service logic element connects to the network.

The mediation point allows the intelligent network provider to customize routing, screening, error handling, and billing functions to suit the operating requirements of the network.

Numerous modifications, variations and adaptations may be made to the particular embodiments of the invention described above without departing from the scope of the invention, which is defined in the claims.

WHAT IS CLAIMED IS:

1. A method of providing mediated access to an intelligent network for service providers, the method comprising the steps of:

providing a mediation point at a boundary of the intelligent network for connection to the service providers;

providing, at the mediation point, a predetermined list of network nodes in the intelligent network to which respective service providers are allowed access;

screening, at the mediation point, a message between a service provider and a network node connecting a subscriber of the service provider to ensure that the network node is on the predetermined list of network nodes the service provider is allowed to access in the intelligent network; and

subsequently, routing messages between the service provider and the network node.

2. A method as claimed in claim 1 further comprising the step of generating billing for any use of the intelligent network by a service provider.

3. A method as claimed in claim 2 wherein the step of routing messages between the service provider and the network node includes the step of, for messages from the network node to the service provider, routing a message from the network node to which the subscriber is connected to the mediation point via a signalling transfer point, where the network node, the mediation point, and the signalling transfer point are within the intelligent network.

4. A method as claimed in claim 3 wherein the step of screening includes screening message format and parameters.

5. A method as claimed in claim 2 wherein the step of routing messages between the service provider and the network node includes the step of, for messages from the service provider to network node, routing a message from the mediation point, via a signalling transfer point, to the network node to which the subscriber is connected, where the network node, the mediation point, and the signalling transfer point are within the intelligent network.

6 A method as claimed in claim 5 wherein the step of screening includes screening message parameters.

7. A method as claimed in claim 1 further comprising the step of detecting error conditions and informing a network management system thereof.

8. A system for providing mediated access to an intelligent network for service providers, the system comprising:

a mediation point at a boundary of the intelligent network having ports for connection to service providers and a predetermined list of network nodes in the intelligent network to which respective service providers are allowed access; and

a plurality of network nodes for connecting subscribers, each having trigger criteria, for each service provider having access thereto, for selecting one of the service providers in response to a subscriber.

9. A system as claimed in claim 8 wherein the mediation point includes a bus, a plurality of query processors connected to the bus, a network interface, connected to the bus, for connecting the mediation point to the intelligent network, a service provider interface, connected to the bus, for connecting the mediation point to a service provider, and a database connected to the bus.

10. A system as claimed in claim 9 wherein the network interface is connected to a signaling transfer point within the intelligent network.

11. A method of providing mediated access to an intelligent network for service providers, the method comprising the steps of:

ensuring that network integrity, security, and reliability are protected in giving a service provider access to the intelligent network;

allowing the service provider access to the intelligent network; and

billing the service provider for gaining access to the intelligent network.

12. A method as claimed in claim 11 wherein access to the intelligent network includes exchanging messages of a predetermined protocol.

13. A method as claimed in claim 12 wherein the step of ensuring that network integrity, security, and reliability are protected includes the step of screening messages to and from the service provider at all functional layers in the message protocol.

14. A method as claimed in claim 13 wherein the message protocol includes signalling system 7 (SS7) protocol.

15. A method as claimed in claim 14 wherein the step of screening messages includes message transfer part (MTP) screening to ensure that the service provider is properly represented to the intelligent network.

16. A method as claimed in claim 14 wherein the step of screening messages includes signal connection and control part (SCCP) screening to ensure that only a service provider

on a predetermined list of network nodes is allowed access to the intelligent network.

17. A method as claimed in claim 14 wherein the step of screening messages includes transaction capabilities application part (TCAP) screening to ensure that the messages conform to a format defined by the protocol.

18. A method as claimed in claim 14 wherein the step of screening messages includes operations screening to ensure that any operation required by a message is of a type provided by the intelligent network.

19. A method as claimed in claim 14 wherein the step of screening messages includes parameter screening to ensure that appropriate parameters are present within the message and that the parameters present have appropriate values.

20. A method as claimed in claim 11 wherein the step of ensuring that network integrity, security, and reliability are protected includes detecting error conditions related to access to the intelligent network by the service provider.

21. A method as claimed in claim 20 wherein the step of detecting error conditions includes the steps of detecting faulty equipment of the service provider and providing a level of service to subscribers of the service provider.

22. A method as claimed in claim 11 wherein the step of allowing the service provider access to the intelligent network includes allowing the service provider to manage data resident in the intelligent network that is related to services offered by the service provider and subscribers of the service provider.

23. A system for providing mediated access for service providers to an intelligent network, the system comprising:

a mediation point at a boundary to the intelligent network and having mediation functions for interconnection of service provider service control points to predetermined service switching points within the network; and

service switching points within the network having mediation functions for interconnection to selected service provider service control points.

24. A system as claimed in claim 23 wherein the mediation point comprises a point of logical interconnection.

25. A system as claimed in claim 23 wherein the mediation point comprises a point of physical interconnection.

26. A system as claimed in claim 23 wherein the interconnection between the service provider service control point and the service switching point includes exchanging messages of a predetermined protocol.

27. A system as claimed in claim 26 wherein the mediation functions of the mediation point comprises routing and screening capabilities and TCAP/AIN application level mediation functions.

28. A system as claimed in claim 26 wherein the mediation functions of the mediation point can be altered with regard to routing, screening, error handling, and billing to suit the operating requirements of the intelligent network

29. A system as claimed in claim 23 further comprising management interfaces, between the service providers and the intelligent network, which allow the service providers to manage data resident in the intelligent network, that is related to the services offer thereby and the subscribers thereof.

F.P. Turpin,
Patent Agent for the Applicants.

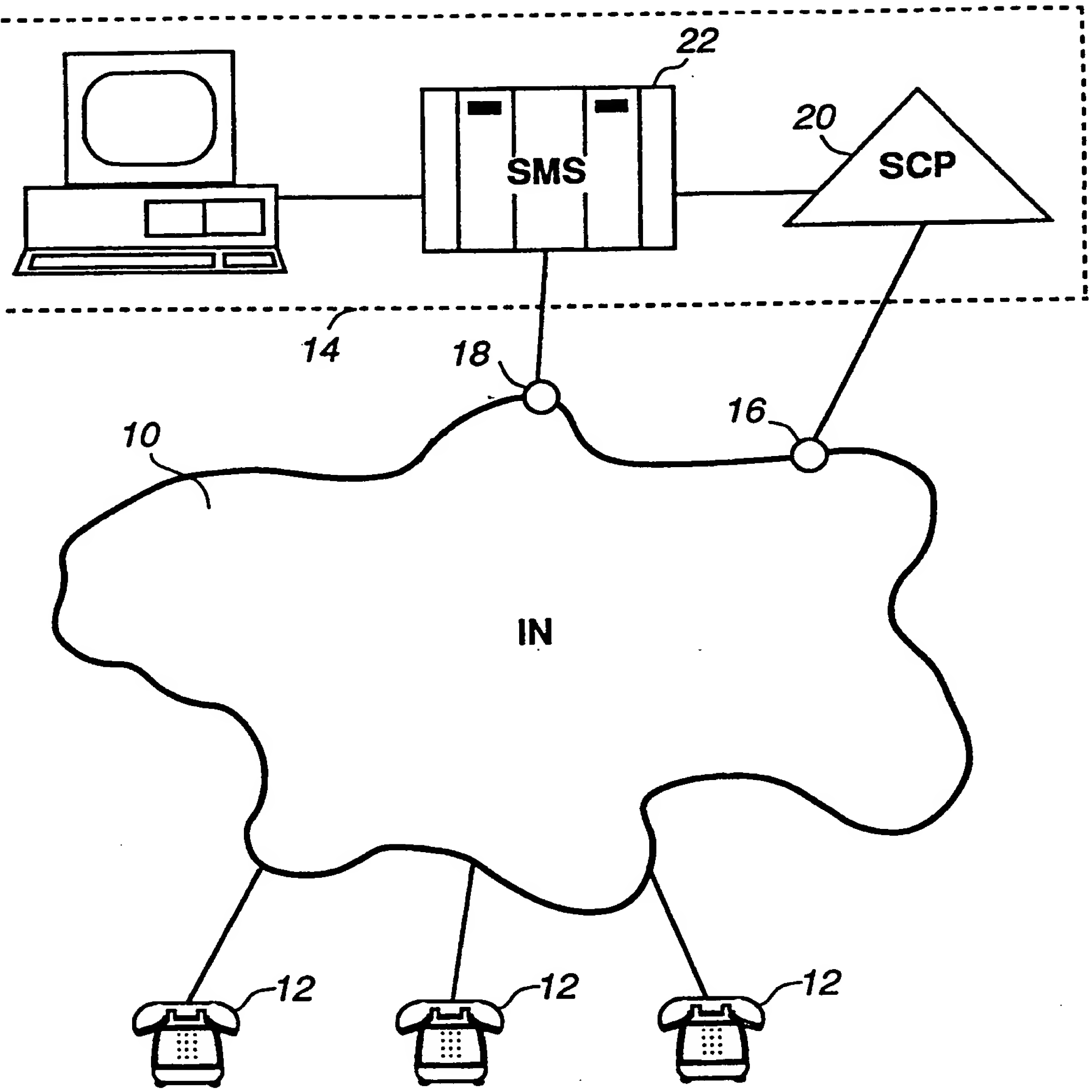


Fig. 1

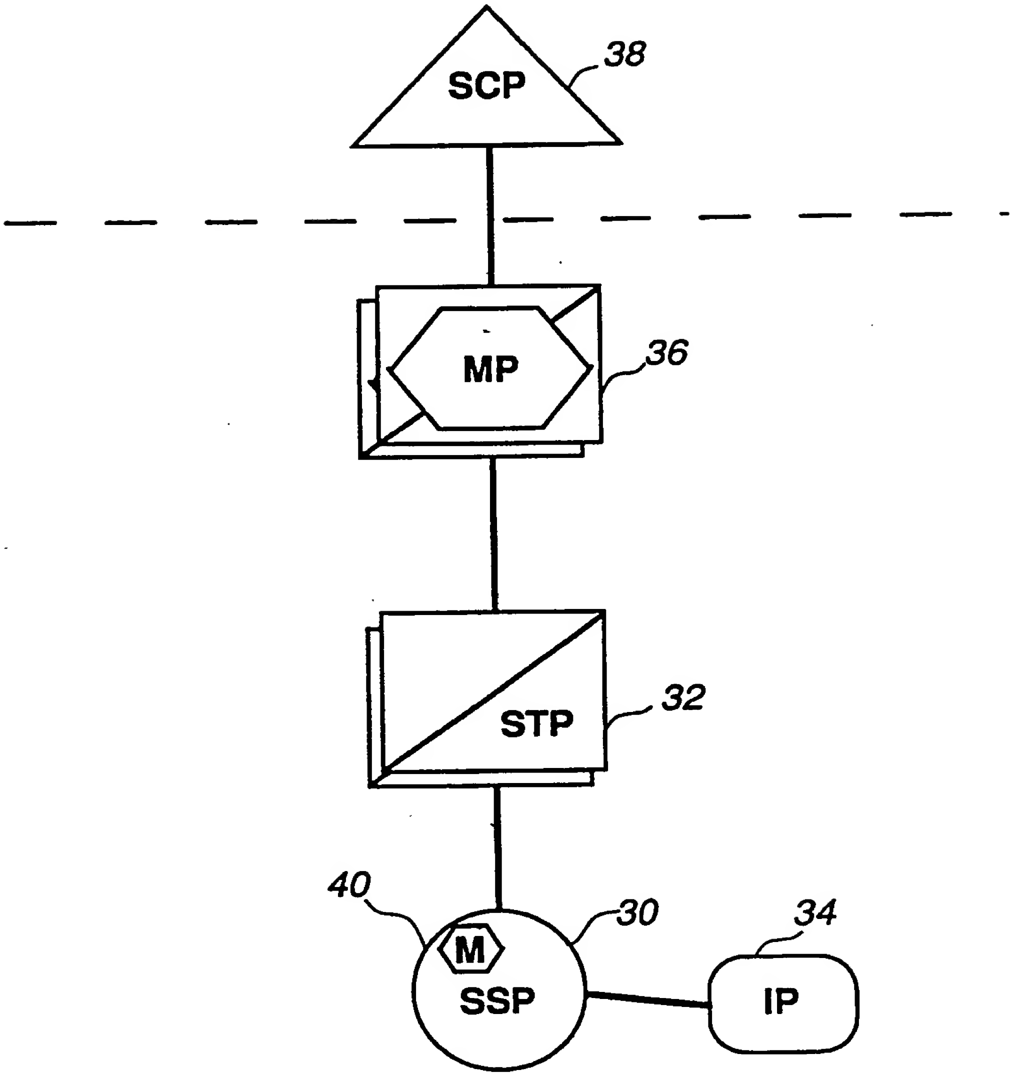
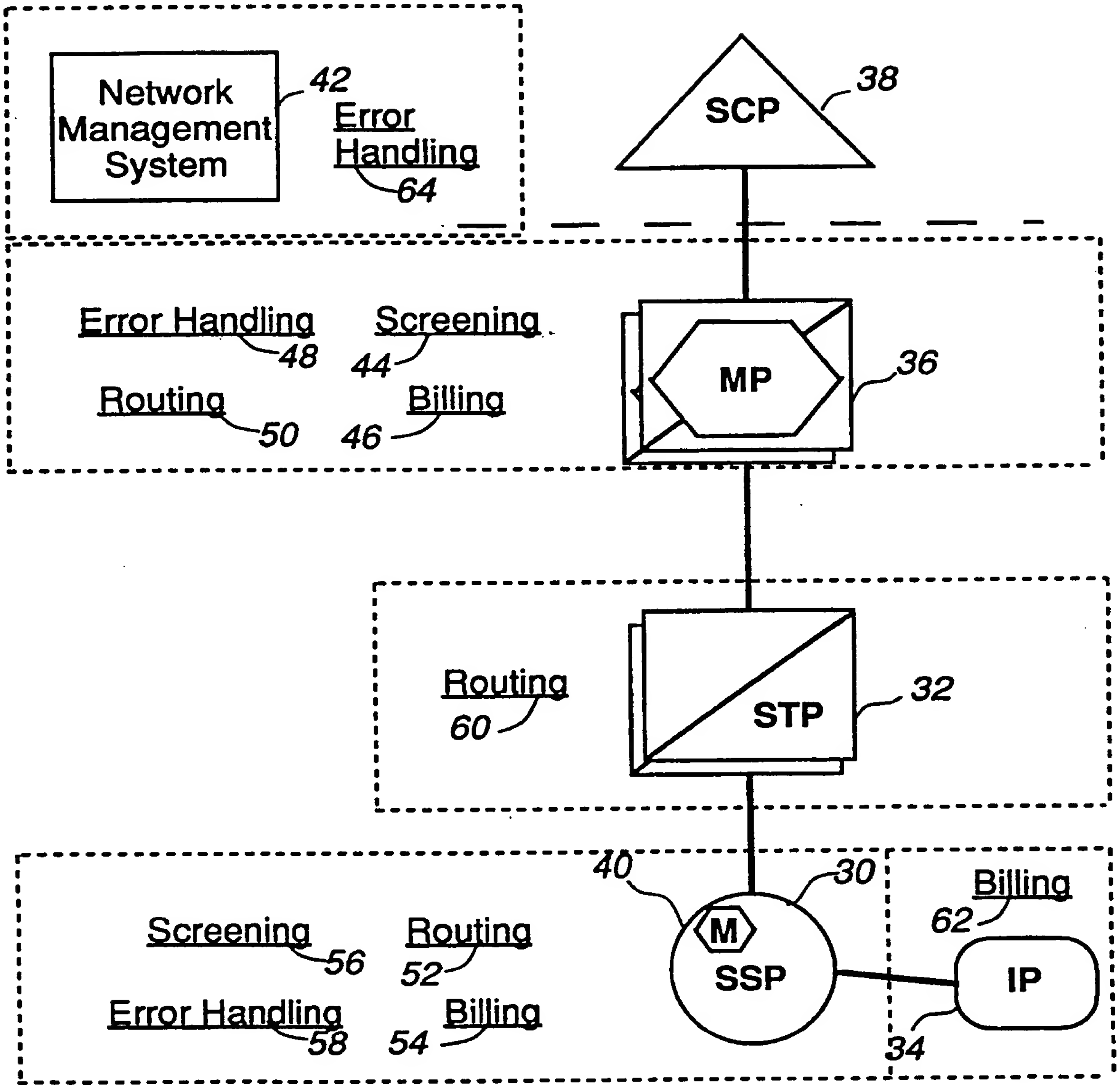


Fig. 2



Network Management System
42
Error Handling
64
SCP
38
Error Handling
48
Screening
44
Routing
50
Billing
46
MP
36
Routing
60
STP
32
40
30
Billing
62
Screening
56
Routing
52
M
SSP
IP
Error Handling
58
Billing
54
34

Fig. 3

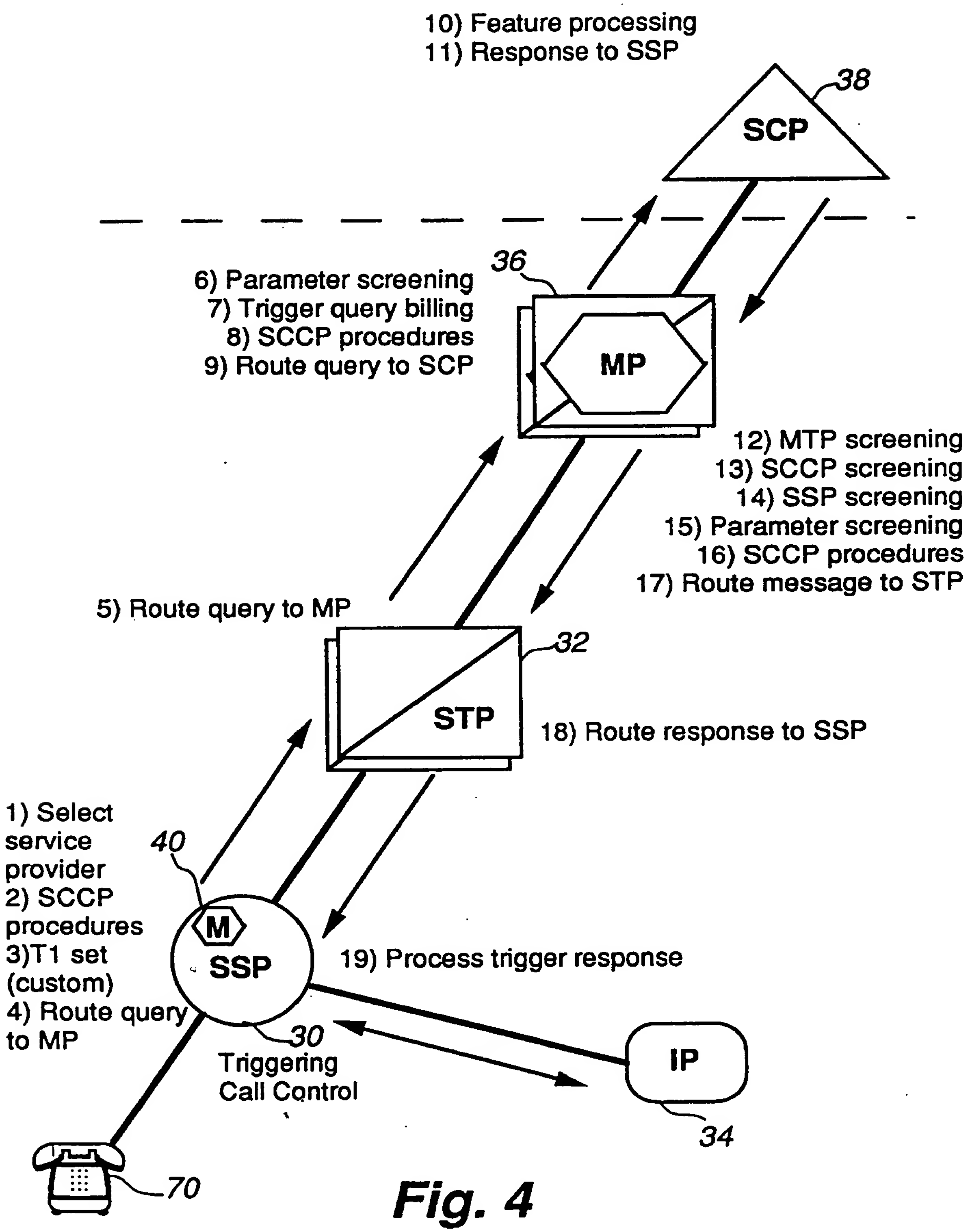

10) Feature processing
11) Response to SSP
38
SCP
36
6) Parameter screening
7) Trigger query billing
8) SCCP procedures
9) Route query to SCP
MP
12) MTP screening
13) SCCP screening
14) SSP screening
15) Parameter screening
16) SCCP procedures
17) Route message to STP
5) Route query to MP
32
STP
18) Route response to SSP
1) Select service provider
2) SCCP procedures
3)T1 set (custom)
4) Route query to MP
40
M
SSP
19) Process trigger response
30
Triggering Call Control
IP
34
70

Fig. 4

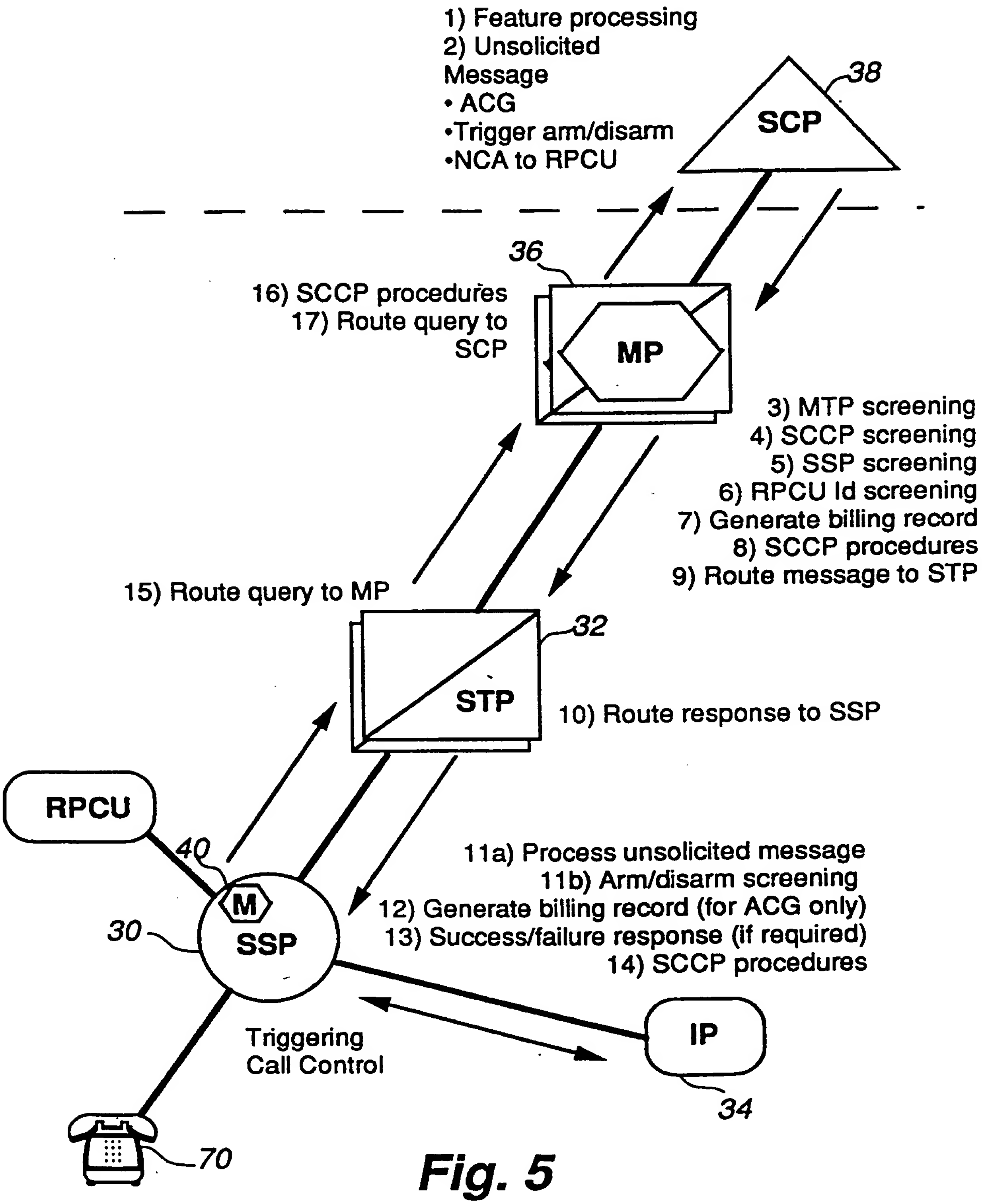

1) Feature processing
2) Unsolicited Message
• ACG
•Trigger arm/disarm
•NCA to RPCU
SCP
38
36
16) SCCP procedures
17) Route query to SCP
MP
3) MTP screening
4) SCCP screening
5) SSP screening
6) RPCU Id screening
7) Generate billing record
8) SCCP procedures
9) Route message to STP
15) Route query to MP
32
STP
10) Route response to SSP
RPCU
40
M
SSP
30
11a) Process unsolicited message
11b) Arm/disarm screening
12) Generate billing record (for ACG only)
13) Success/failure response (if required)
14) SCCP procedures
Triggering Call Control
IP
34
70

Fig. 5

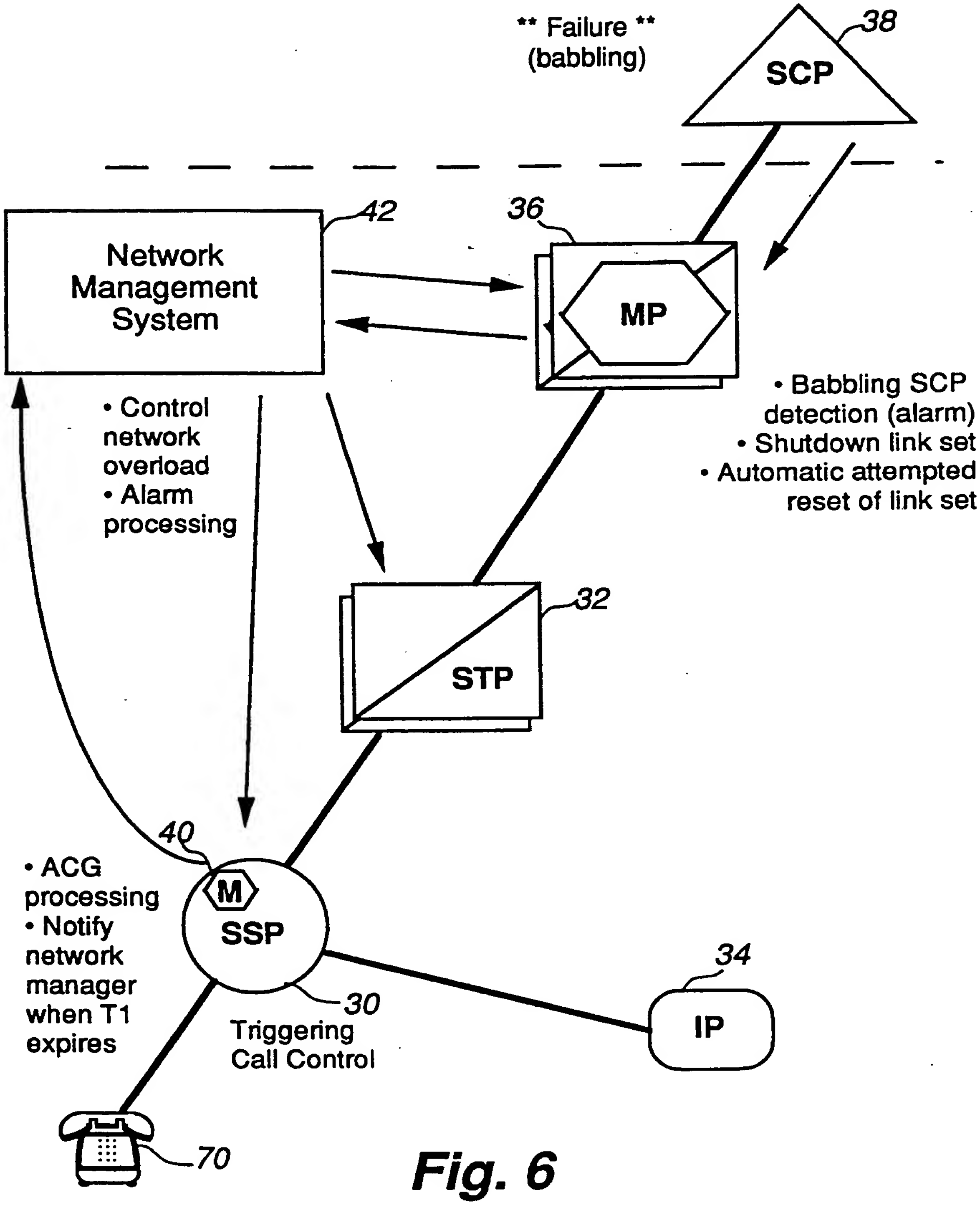

** Failure **
(babbling)
SCP
38
Network
Management
System
42
36
MP
• Babbling SCP
detection (alarm)
• Shutdown link set
• Automatic attempted
reset of link set
• Control
network
overload
• Alarm
processing
STP
32
40
M
SSP
• ACG
processing
• Notify
network
manager
when T1
expires
30
Triggering
Call Control
34
IP
70

Fig. 6

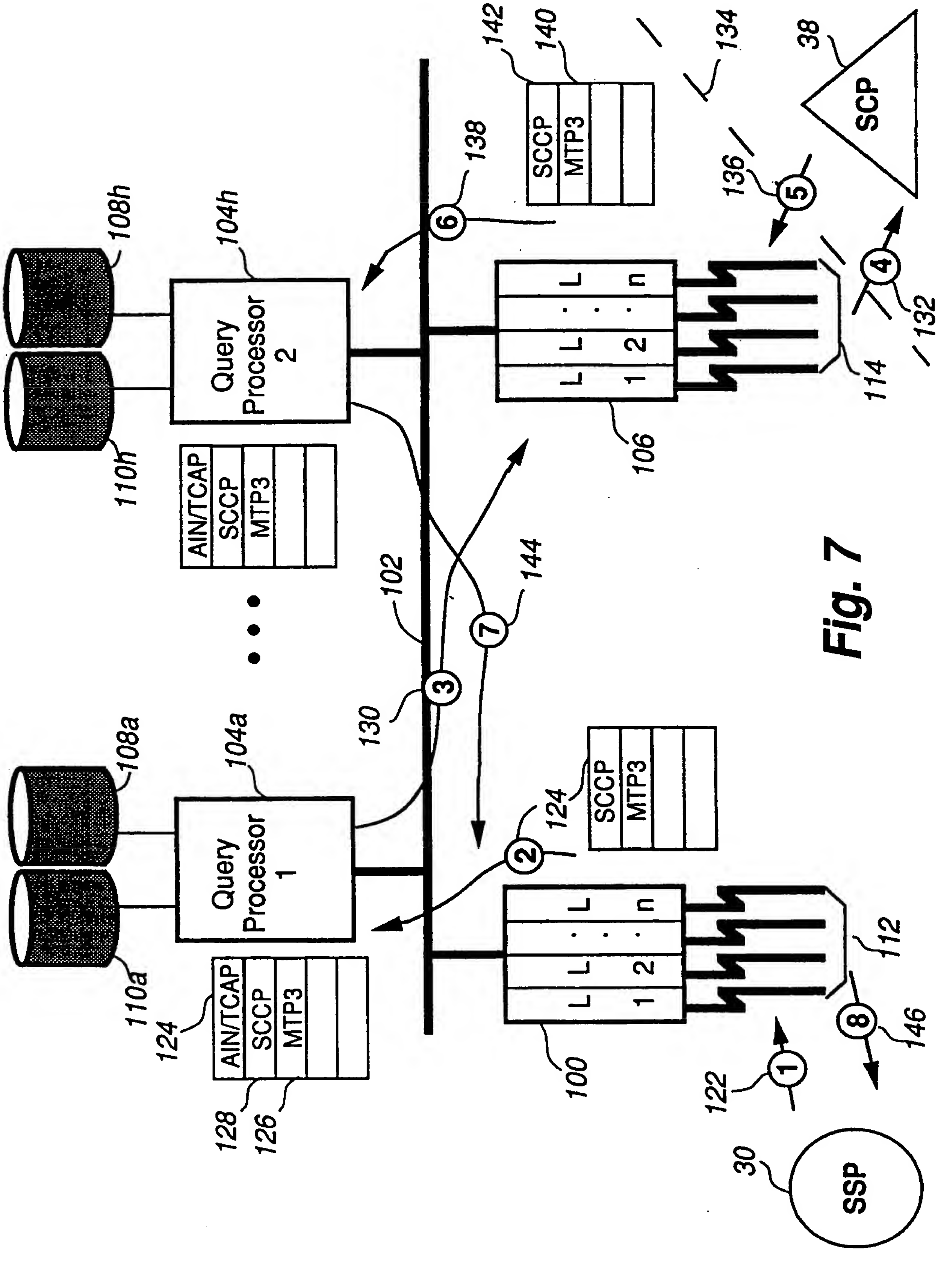

SSP
30
SCP
38
Query Processor 1
Query Processor 2
104a
104h
108a
110a
108h
110h
AIN/TCAP
SCCP
MTP3
124
128
126
SCCP
MTP3
124
SCCP
MTP3
142
140
L
L
1
2
n
100
106
112
114
102
130
144
138
136
134
132
122
146
1
2
3
4
5
6
7
8

Fig. 7